



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/032,722

10/27/2001

Shigeki Kamiya

450100-03253.1

6409

20999 7590 03/21/2007
FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER

HENNING, MATTHEW T

ART UNIT

PAPER NUMBER

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
--	-----------	---------------

3 MONTHS

03/21/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/032,722

Applicant(s)

KAMIYA ET AL.

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 January 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5-8, 10-13, 15-18, 20-23 and 25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5-8, 10-13, 15-18, 20-23 and 25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Art Unit: 2131

1 This action is in response to the communication filed on 1/3/2007.

2 **DETAILED ACTION**

3 ***Response to Arguments***

4 Applicant's arguments with respect the claims have been considered but are moot in view
5 of the new ground(s) of rejection.

6 Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 have been examined.

7 All objections and rejections not presented below have been withdrawn.

8 ***Claim Rejections - 35 USC § 103***

9 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
10 obviousness rejections set forth in this Office action:

11 *A patent may not be obtained though the invention is not identically disclosed or*
12 *described as set forth in section 102 of this title, if the differences between the subject matter*
13 *sought to be patented and the prior art are such that the subject matter as a whole would have*
14 *been obvious at the time the invention was made to a person having ordinary skill in the art to*
15 *which said subject matter pertains. Patentability shall not be negated by the manner in which*
16 *the invention was made.*
17

18 Claims 1-3, 5-8, 10-13, 15-18, and 20 are rejected under 35 U.S.C. 103(a) as being
19 unpatentable over Rosner et al. (US Patent Number 6,636,968) hereinafter referred to as Rosner,
20 and further in view of Kato (US Patent Number 6,381,331), and further in view of Schneier
21 ("Applied Cryptography").

22 Regarding claim 1, Rosner disclosed a digital data delivery method for use in delivering
23 digital data from all upstream system to a downstream system, said upstream system providing
24 multipoint delivery of encrypted digital data to specific destinations, and said downstream
25 system decrypting the delivered digital data (See Rosner Fig. 2 and Col. 4 Paragraph 3), said

Art Unit: 2131

1 method comprising the steps of: encrypting digital data by said upstream system using an
2 encryption key (See Rosner Col. 3 Lines 42-45); generating a plurality of pieces of key
3 information on the basis of said encryption key, respective pieces of said key information being
4 specific to each of said specific destinations (See Rosner Col. 3 Lines 48-57); delivering said
5 respective pieces of key information to each of said specific destinations (See Rosner Col. 3 Line
6 57 – Col. 4 Line 7); delivering the encrypted digital data (See Rosner Col. 3 Lines 8-10);
7 restoring said encryption key by said downstream system using said respective pieces of key
8 information (See Rosner Col. 4 Lines 8-12); and using the restored encryption key to decrypt the
9 encrypted digital data (See Rosner Col. 4 Lines 12-17), but Rosner failed to disclose generating
10 the pieces of key information by dividing the encryption key by a unique division pattern, the
11 division pattern based on the content of said digital data, or that the key information was
12 delivered over a plurality of delivery routes which differ from routes for delivering said digital
13 data and which are further different from each other.

14 Kato teaches that in an content sending system, in order to prevent the content from being
15 repetitively gotten without approval, the encryption keys used to encrypt the content should be
16 prepared for each content (See Kato Col. 10 Lines 37-52).

17 Schneier teaches that key information should be delivered over a different
18 communication channel than the data encrypted using the key information (See Schneier Col.
19 Page 176 Lines 34-37). Schneier further teaches that keys should be split and each part should
20 be delivered over a separate channel (See Schneier Page 177 Paragraph 1). Schneier further
21 teaches that the key should be split using random numbers, which would be unique for each
22 splitting (See Schneier Pages 70-71 Section 3.6 Secret Splitting).

Art Unit: 2131

1 It would have been obvious to the ordinary person skilled in the art at the time of
2 invention to employ the teachings of Kato in the delivery system of Rosner, by providing each
3 content with its own encryption key. This would have been obvious because the ordinary person
4 skilled in the art would have been motivated to prevent a recipient from decrypting multiple
5 contents without approval. It further would have been obvious to the ordinary person skilled in
6 the art at the time of invention to employ the teachings of Schneier in the partial key delivery
7 system of Rosner by splitting and delivering the partial keys and group key used to reconstruct
8 the decryption key over different channels and further over a different channel than the encrypted
9 content. This would have been obvious because the ordinary person skilled in the art would have
10 been motivated to protect the key from being illicitly reconstructed as well as to protect the
11 encrypted content from being illicitly decrypted. In this combination, it would be obvious that
12 when the key is updated for each content, the key splitting would be repeated and a new random
13 number would be generated for the splitting. Therefore, it would be obvious that in this
14 combination, the division pattern would vary for the content that it was associated with, and as
15 such the division pattern would be "based" on the content.

16 Claim 2 is rejected for the same reasons as claim 1 above and further because the
17 passkeys of claim 2 are equivalent to the pieces of key information of claim 1 above.

18 Regarding claim 3, the combination of Rosner, Kato, and Schneier disclosed a digital
19 data delivery method for use in delivering digital data from an upstream system to a downstream
20 system, said upstream system providing multipoint delivery of encrypted digital data to specific
21 destinations, and said downstream system decrypting the delivered digital data (See Rosner Fig.
22 2 and Col. 4 Paragraph 3), said method comprising the steps of: encrypting digital data by said

Art Unit: 2131

1 upstream system using an encryption key (See Rosner Col. 3 Lines 42-45); generating on the
2 basis of said encryption key, a set of passkeys by dividing said encryption key by a division
3 pattern unique to each of said specific destinations and based on the content of said digital data
4 (See the rejection of claim 1 above); generating a plurality of partial keys based on a portion of
5 the passkeys in said set or a portion of passkey information from which said passkeys may be
6 reproduced (See Rosner Col. 3 Lines 48-57 especially elements 225-227); delivering either said
7 plurality of partial keys or partial key information, from which said partial keys may be
8 reproduced (See Rosner Col. 3 Lines 57-60), and delivering the remaining passkeys not used to
9 generate said partial keys or the remaining passkey information (See Rosner Fig. 2 which clearly
10 depicts element 212a being transmitted from the source to the destination devices and Fig. 4
11 further confirms this), to each of said specific destinations over a plurality of delivery routes
12 which differ from routes for delivering said digital data and which are further different from each
13 other (See the rejection of claim 1 above); delivering the encrypted digital data (See Rosner Col.
14 3 Lines 8-10); restoring said encryption key by using said downstream system using either said
15 plurality of partial keys or said partial key information and using either said remaining passkeys
16 or said remaining passkey information delivered over said plurality of delivery routes (See
17 Rosner Col. 4 Lines 8-12); and using the restored encryption key to decrypt the encrypted digital
18 data (See Rosner Col. 4 Lines 12-17).

19 Regarding claim 5, the combination of Rosner, Kato, and Schneier disclosed a digital
20 data delivery method for use in delivering digital data from an upstream system to a downstream
21 system, said upstream system providing multipoint delivery of encrypted digital data to specific
22 destinations, and said downstream system decrypting the delivered digital data (See Rosner Fig.

Art Unit: 2131

1 2 and Col. 4 Paragraph 3), said method comprising the steps of: encrypting digital data by said
2 upstream system using a first encryption key (See Rosner Col. 3 Lines 42-45); generating a
3 second encryption key specific to each of said specific destinations and/or to said digital data
4 (See Rosner Col. 6 Lines 23-25); using said second encryption key to encrypt either said first
5 encryption key or first encryption key information from which said first encryption key may be
6 reproduced (See Rosner Col. 4 Lines 55-59 Element 212a and Fig. 3 Element 'X'); generating,
7 on the basis of said second encryption key, a set of passkeys (See Rosner Col. 4 Lines 55-59
8 Elements 225-228) by dividing said encryption key by a division pattern unique to each of said
9 specific destinations and based on the content of said digital data (See the rejection of claim 1
10 above); delivering either said encrypted first encryption key or said encrypted first encryption
11 key information and delivering either said set of passkeys or passkey information, from which
12 said set of passkeys may be reproduced (See Rosner Col. 3 Lines 57-67), to each of said specific
13 destinations over a plurality of delivery routes which differ from routes for delivering said digital
14 data and which are further different from each other (See the rejection of claim 1 above);
15 delivering the encrypted digital data (See Rosner Col. 3 Lines 8-10); restoring said second
16 encryption key by using either said set of passkeys or said passkey information delivered over
17 said plurality of delivery routes so as to decrypt either said first encryption key or said first
18 encryption key information and thereby restore said first encryption key (See Rosner Col. 4
19 Lines 8-12); and decrypting the encrypted digital data by use of the restored first encryption key
20 (See Rosner Col. 4 Lines 12-17).

21 Claims 6, 11, and 16 are rejected for the same reasons as claim 1 above and further
22 because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Claims 8, 13, and 18, are rejected for the same reasons as claim 3 above and further because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Claims 10, 15, and 20, are rejected for the same reasons as claim 5 above and further because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Claims 21-23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Rosner, Kato, and Schneier as applied to claims 1-5 above, and further in view of Schneier.

The combination of Rosner and Schneier disclosed a system and method for communicating encrypted data using key reconstruction at the receiver (See the rejections of claims 1-5 above), but failed to disclose software for implementing the method.

Schneier teaches that any encryption algorithm can be implemented in software (See Schneier Page 225 Lines 25-38).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the encryption system of Rosner and Schneier by providing software to implement the encryption method. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide flexibility and portability, ease of use, and ease of upgrade to the encryption system.

Conclusion

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 have been rejected.

Art Unit: 2131

1 The prior art made of record and not relied upon is considered pertinent to applicant's
2 disclosure.

3 Applicant's amendment necessitated the new ground(s) of rejection presented in this
4 Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

5 Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


6 A shortened statutory period for reply to this final action is set to expire THREE
7 MONTHS from the mailing date of this action. In the event a first reply is filed within TWO
8 MONTHS of the mailing date of this final action and the advisory action is not mailed until after
9 the end of the THREE-MONTH shortened statutory period, then the shortened statutory period
10 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37
11 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,
12 however, will the statutory period for reply expire later than SIX MONTHS from the date of this
13 final action.

14 Any inquiry concerning this communication or earlier communications from the
15 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
16 The examiner can normally be reached on M-F 8-4.

17 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
18 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
19 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent
2 Application Information Retrieval (PAIR) system. Status information for published applications
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
4 applications is available through Private PAIR only. For more information about the PAIR
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would
7 like assistance from a USPTO Customer Service Representative or access to the automated
8 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

9
10
11
12
13
14
15 
16 Matthew Henning
17 Assistant Examiner
18 Art Unit 2131
3/17/2007

CHRISTOPHER REVAK
PRIMARY EXAMINER

